

IN THE CLAIMS

The following is a listing of the claims in the application with claims 1-18 and claims 21-42 shown as amended and with claims 19-20 cancelled and claims 49-53 added as new claims.

LISTING OF CLAIMS

1. (currently amended) Method for ~~matching pairing~~ digital data reception equipment (2) with a plurality of external security modules (6, 8) each with a unique identifier, method characterised in that it comprises the following steps:

- connecting an external security module (6, 8) to the reception equipment, and
- memorizing, on the fly, the unique identifier of the connected security module (6, 8) in the reception equipment (2), on the fly.

2. (currently amended) Method ~~set forth in according to~~ claim 1, characterised in that it also includes a ~~check phase verification phase~~ consisting of verifying whether or not the identifier of said module is memorised in reception equipment (2), every time that an external security module (6, 8) is connected to this reception equipment (2) later on.

3. (currently amended) Method ~~set forth in according to~~ claim 2, characterised in that it also comprises a step of transmitting a signal to the reception equipment (2) including at least one message to manage memorisation of the identifier of the external security module (6, 8) and/or a ~~check phase management message message to manage a verification phase~~.

4. (currently amended) Method ~~set forth in according to~~ claim 3, characterised in that said signal includes at least one of the following set values instructions:

- authorise authorizing memorisation,
- prohibit prohibiting memorisation,
- erase erasing identifiers previously memorised in the reception equipment (2),
- activate activating or deactivating the check verification phase.

5. (currently amended) Method ~~set forth in~~ according to claim 3, characterised in that said signal also includes an indication as to the maximum allowable number of memorised identifiers.

6. (currently amended) Method ~~set forth in~~ according to claim 3, characterised in that said signal includes a reconfiguration ~~set value~~ instruction through which an updated list of identifiers of external security modules (6, 8) ~~matched~~ paired with the reception equipment(2) equipment (2) is transmitted to said reception equipment (2).

7. (currently amended) Method ~~set forth in~~ according to claim 6, characterised in that said list is transmitted directly to the reception equipment (2).

8. (currently amended) Method ~~set forth in~~ according to claim 6, characterised in that said list is transmitted through an external security module (6, 8) connected to said reception equipment (2).

9. (currently amended) Method ~~set forth in~~ according to claim 2, in which said ~~check phase verification phase~~ includes a procedure consisting of disturbing the data processing if the identifier of the connected external security module (6, 8) is not previously memorised in the reception equipment (2).

10. (currently amended) Method ~~set forth in~~ according to claim 1, characterised in that said ~~data are distributed~~ data are either unencrypted or encrypted without encryption or scrambled by means of an encrypted control word and in that each external security module (6, 8) includes access rights to said data and a decryption algorithm for said control word.

11. (currently amended) Method ~~set forth in one of claims 4 or 5 according to claim 4,~~ characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to an external security module (6, 8) associated with ~~this~~ said reception equipment (2).

12. (currently amended) Method set forth in according to one of claims 4 or 5 claim 4, characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to this said reception equipment (2).

13. (currently amended) Method set forth in according to claim 6, characterised in that for a given reception equipment (2) said list is transmitted in an EMM message specific to a security module (6, 8) associated with this reception equipment (2).

14. (currently amended) Method set forth in according to claims claim 4 or 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (2).

15. (currently amended) Method set forth in one of according to claims claim 4 or 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (2).

16. (currently amended) Method set forth in according to claim 6, characterised in that for a given group of reception equipment (2), said updated list of identifiers of external security modules (6, 8) is transmitted in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (2).

17. (currently amended) Method set forth in one of according to claims claim 4 or 5, characterised in that the message for managing the verification phase check signal is transmitted to a group of reception equipment (2) in a private flow to a group of reception equipment (2) processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment.

18. (currently amended) Method set forth in according to claim 6, characterised in that for a given group of reception equipment (2), said updated list of identifiers of external security modules (6, 8) is transmitted in a private flow to each reception equipment (2) in a private flow processed by a dedicated software executable in each reception equipment as

a function of the identifier of the external security module associated with said reception equipment.

19 – 20 (cancelled).

21. (currently amended) Method ~~set forth in one of according to claims~~ claim 11 to 13, characterised in that said EMM are in the following format contain messages with the following structure:

EMM-U_section()	{
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

22. (currently amended) Method ~~set forth in one of claims~~ according to claim 14 to 16, characterised in that said EMM is specific to all external security modules (6, 8) or to all reception equipment (2) and are in contain messages with the following format structure:

EMM-G_section()	{
table_id = 0x8A or 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved 1 bit	
ISO_reserved 2 bits	
EMM-G_section_length	12 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

23. (currently amended) Method set forth in one of claims according to claim 14 to 16, characterised in that said EMM is specific to a sub-group of external security modules (6, 8) or reception equipment (2) and are in contain messages with the following format structure:

```

EMM-S_section() {
    table_id = 0x8E 8 bits
    section_syntax_indicator = 0           1 bit
    DVB_reserved 1 bit
    ISO_reserved 2 bits
    EMM-S_section_length          12 bits
    shared_address_field        24 bits
    reserved                   6 bits
    data_format     1 bit
    ADF_scrambling_flag      1 bit
    for (i=0; i<N; i++) {
        EMM_data_byte          8 bits
    }
}

```

24. (currently amended) Method set forth in according to claim 1, characterised in that identifiers of external security modules (6, 8) are grouped in an encrypted list.

25. (currently amended) Method set forth in any one of claims according to claim 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised, and in that matching pairing is done between said decoder and said card (6).

26. (currently amended) Method set forth in any one of claims according to claim 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory that can cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching pairing is done between said decoder and said removable security interface (8).

27. (currently amended) Method ~~set forth in any one of claims according to claim 1 to 24~~, characterised in that the reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory that can cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), and in that matching pairing is done between said removable security interface (8) and said access control cards (6).

28. (currently amended) Method ~~set forth in according to~~ claim 10, characterised in that the data are audiovisual programs.

29. (currently amended) Reception equipment (2) that can be matched paired with a plurality of external security modules (6, 8) to manage access to digital data distributed by an operator, characterised in that it includes means of for memorising memorizing on the fly, the identifier of each external security module (6, 8) connected to it, on-the-fly said reception equipment.

30. (currently amended) Equipment ~~Reception equipment set forth in according to~~ claim 29, characterised in that it comprises a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, matching pairing being done between said decoder and said card (6).

31. (currently amended) Equipment ~~set forth in Reception equipment according to~~ claim 29, characterised in that it includes a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and that is designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching pairing being done between said decoder and said removable security interface (8).

32. (currently amended) Equipment set forth in Reception equipment according to claim 29, characterised in that it includes a decoder provided with a removable security interface (8) with a non-volatile memory and that is designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards (6) and in that matching pairing is done between said removable security interface (8) and said access control cards (6).

33. (currently amended) Decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a unique identifier and including at least one data processing algorithm, decoder characterised in that it includes means of memorising for memorizing, on the fly, the identifier of each external security module (6, 8) connected to it, on the fly said decoder.

34. (currently amended) Decoder set forth in according to claim 33, characterised in that said external security modules (6, 8) are access control cards (6) in which are stored information about access rights of a subscriber to digital data distributed by an operator are stored.

35. (currently amended) Decoder set forth in according to claim 33, characterised in that said external security modules (6, 8) are removable security interfaces (8) including a non-volatile memory that can cooperate firstly with the decoder and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator.

36. (currently amended) Reception equipment comprising a Removable removable security interface (8) including a non-volatile memory and designed to cooperate firstly with a reception equipment (2), and secondly with a plurality of conditional access control cards (6), to manage access to digital data distributed by an operator, each card (6) having a unique identifier and containing information about access rights of a subscriber to said digital data, with said removable security interface characterised in that it includes means of for recording the identifier of each access control card (6) in said non-volatile memory, on the fly.

37. (currently amended) ~~Removable security Interface set forth in Reception equipment according to claim 36, characterised in that it consists of a PCMCIA card on which is installed digital data descrambling software is installed.~~

38. (currently amended) ~~Removable security Interface set forth in Reception equipment according to claim 36, characterised in that it consists of a software module.~~

39. (currently amended) Executable computer program stored in a computer readable medium of in a reception equipment (2) that can cooperate with a plurality of external security modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, characterised in that it includes instructions to memorise for executing the memorization, on the fly, of the identifier of each external security module (6, 8) connected to said reception equipment (2), on the fly.

40. (currently amended) Computer program set forth in according to claim 39, characterised in that it also includes instructions to for locally generate matching generating pairing control parameters of the reception equipment (2) with an external security module (6, 8) as a function of a signal transmitted to said reception equipment (2) by the operator.

41. (currently amended) Computer program set forth in according to claim 39, characterised in that it also includes instructions intended to check for checking if the identifier of said external security module (6, 8) is memorised in the reception equipment (2), at each later use of an external security module (6, 8) with the reception equipment (2).

42. (currently amended) System including a plurality of reception equipment (2) connected to a data and/or services broadcasting network, each reception equipment (2) being capable of being matched adapted to be paired with a plurality of external security modules (6, 8), said system also including a commercial management platform (1) communicating with the reception equipment (2) and with said external security modules (6, 8) characterised in that it also includes:

- a first module arranged in said commercial management platform (1) and that will generate matching pairing queries,

- and a second security module arranged in said reception equipment (2) that will process said queries to prepare a matching pairing configuration and to control matching pairing.

43. (new) Method according to claim 5, characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to an external security module (6; 8) associated with said reception equipment (2).

44. (new) Method according to claim 5, characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to this said reception equipment (2).

45. (new) Method set forth in claim 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (2).

46. (new) Method set forth in claim 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (2).

47. (new) Method set forth in claim 5, characterised in that the message for managing the verification phase is transmitted to a group of reception equipment (2) in a private flow processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment.

48. (new) Method set forth in claim 12, characterised in that said EMM contain messages with the following format:

EMM-U_section()	{
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

49. (new) Method set forth in claim 13, characterised in that said EMM contain messages with the following format:

EMM-U_section()	{
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

50. (new) Method set forth in claim 15, characterised in that said EMM is specific to all external security modules (6, 8) or to all reception equipment (2) and contain messages with the following structure:

EMM-G_section()	{
table_id = 0x8A or 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved 1 bit	
ISO_reserved 2 bits	
EMM-G_section_length	12 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

51. (new) Method set forth in claim 16, characterised in that said EMM is specific to all external security modules (6, 8) or to all reception equipment (2) and contain messages with the following structure:

```

EMM-G_section() {
    table_id = 0x8A or 0x8B           8 bits
    section_syntax_indicator = 0      1 bit
    DVB_reserved 1 bit
    ISO_reserved 2 bits
    EMM-G_section_length            12 bits
    for (i=0; i<N; i++) {
        EMM_data_byte               8 bits
    }
}

```

52. (new) Method set forth in claim 15, characterised in that said EMM is specific to a sub-group of external security modules (6, 8) or reception equipment (2) and contain messages with the following structure:

```

EMM-S_section() {
    table_id = 0x8E 8 bits
    section_syntax_indicator = 0      1 bit
    DVB_reserved 1 bit
    ISO_reserved 2 bits
    EMM-S_section_length            12 bits
    shared_address_field            24 bits
    reserved                         6 bits
    data_format          1 bit
    ADF_scrambling_flag             1 bit
    for (i=0; i<N; i++) {
        EMM_data_byte               8 bits
    }
}

```

53. (new) Method set forth in claim 16, characterised in that said EMM is specific to a sub-group of external security modules (6, 8) or reception equipment (2) and contain messages with the following structure:

```
EMM-S_section() {
    table_id = 0x8E 8 bits
    section_syntax_indicator = 0           1 bit
    DVB_reserved 1 bit
    ISO_reserved 2 bits
    EMM-S_section_length                 12 bits
    shared_address_field                24 bits
    reserved                           6 bits
    data_format      1 bit
    ADF_scrambling_flag                1 bit
    for (i=0; i<N; i++) {
        EMM_data_byte                  8 bits
    }
}
```